Mathematical model of legal regulation of the spread of information influences in social networks

Oleksandr Tkachenko[1,2,*,†], Anna Ilyenko[2,†], Yelyzaveta Meleshko[1,†], Oleksandr Ulichev[1,†] and Henryk Noga[3,†]

[1]*Central Ukrainian National Technical University, Universytetskyi Ave., 8, Kropyvnytskyi, 25000, Ukraine*
[2]*State University "Kyiv Aviation Institute", Liubomyra Huzara Ave., 1, Kyiv, 03058, Ukraine*
[3]*University of the National Education Commission, Podchorazych Str., 2, Krakow, 30-084, Poland*

Abstract

This paper presents a theoretical mathematical model for the legal regulation of information flows in social networks, aiming to balance freedom of speech with public safety and national security. The model introduces regulation as a variable that affects key societal indicators and enables simulation-based optimization to prevent both excessive censorship and information disorder. It incorporates contextual risk factors such as disinformation levels, user behavior history, geolocation, and event timing to dynamically assess the impact of regulation. Although the model shows promising conceptual potential, it remains primarily theoretical. No empirical data from real social networks have been utilized; all experiments are based on simulated scenarios. This limitation is explicitly acknowledged. Future work should focus on empirical validation using open-source or synthetic datasets and on adapting the model to different socio-cultural and legal contexts. The presented framework lays the foundation for practical tools in digital policymaking to support efforts aimed at maintaining a fair and secure information environment.

Keywords

social media, information influence, legal regulation, disinformation, cybersecurity, data protection, freedom of speech, platform liability, international standards, information security

1. Introduction

In today's information society, social media platforms play a crucial role in shaping public opinion, political processes, and national security [1]. On the one hand, they enable the free exchange of ideas, foster the democratization of the information space, and facilitate the exercise of freedom of speech. On the other hand, these platforms serve as a medium for spreading harmful content, disinformation, and propaganda that can compromise public safety and threaten national interests.

This dual nature creates an urgent need for legal mechanisms that strike a balance between protecting fundamental human rights and safeguarding society against potential threats. To achieve such a balance, an integrated approach is required that can quantitatively assess the impact of various levels of legal regulation on social processes. The proposed mathematical model establishes functional dependencies that describe how indices such as freedom of speech, public safety, and the protection of national interests change in response to regulatory measures, while also accounting for the influence of harmful information flows.

Accordingly, this study aims to develop a mathematical tool for analyzing and optimizing legal regulation in the digital era—a task of great relevance today, as the speed of information dissemination demands new approaches to ensuring national security without undermining freedom of expression.

CH&CMiGIN'25: Fourth International Conference on Cyber Hygiene & Conflict Management in Global Information Networks, June 20–22, 2025, Kyiv, Ukraine
*Corresponding author.
†These authors contributed equally.
alexsunnik@gmail.com (O. Tkachenko); anna.ilienko@npp.nau.edu.ua (A. Ilyenko); elismeleshko@gmail.com (Y. Meleshko); askin79@gmail.com (O. Ulichev); henryk.noga@up.krakow.pl (H. Noga)
0009-0008-1721-3455 (O. Tkachenko); 0000-0001-8565-1117 (A. Ilyenko); 0000-0001-8791-0063 (Y. Meleshko); 0000-0003-3736-9613 (O. Ulichev); 0000-0001-7073-3443 (H. Noga)

2. Background

Current research on mathematical modeling of legal regulation in the context of social networks reveals that while no comprehensive models have been developed specifically for legal regulation, there has been considerable work on related topics, particularly in modeling information influence, misinformation, and social dynamics on digital platforms. Many of these studies employ epidemiological models, fractional-order systems, or power-law-based graph theory to examine the diffusion of news, rumors, and social interactions. These approaches provide valuable foundations for developing future models that incorporate regulatory mechanisms, especially those seeking to quantify and simulate the effects of legal interventions.

For instance, O. S. Ulichev investigates information influence dissemination in social networks within the framework of information confrontation. His work presents a mathematical model that accounts for diverse behavioral strategies of network nodes, addressing the gap in existing models that often overlook individual node behavior [2].

Joydip Dhar, Ankur Jain, and Vijay K. Gupta (2016) propose a mathematical model that applies epidemiological techniques to describe the spread of news and rumors. They introduce detection criteria for rumors and incorporate media awareness as a control strategy to limit rumor dissemination [3].

Michael Muhlmeyer and Shaurya Agarwal (2021), in their book Information Spread in a Social Media Age, provide a comprehensive overview of how information influence spreads across social media and how social networks operate in general [4].

Y. Nakonechna presents a mathematical model that employs the RnSIR framework to describe the spread of information concealment, integrating both user behavior and regulatory restrictions. This model is useful for simulating scenarios involving information manipulation or concealment in cyberspace [5].

Khrapov and Stolbova utilize an extended SIR model to analyze comment dynamics on Facebook posts, offering analytical insights into public reaction and information virality on social media platforms [6].

Expanding these approaches, Meira Shur-Ofry and Gadi Fibich (2019) explore how legal innovations spread by applying diffusion models, suggesting that legal norms propagate similarly to cultural ideas within a network and are influenced by structural and informational factors [7].

W. Huleihel and Y. Refael (2024) propose a mathematical audit framework for assessing influence on social media, incorporating legal obligations and ethical standards into the quantification of digital influence [8].

Zhu, Guan, and Zhang (2020) introduce a delayed rumor propagation model in complex networks, which reflects real-world delays in rumor spread and public response. Their model can be extended to include points where legal regulation may intervene [9].

El Bhih, Yaagoub, Rachik, and Allali (2024) develop a system of differential equations to simultaneously model the spread of rumors and counter-rumors, allowing simulation of regulatory responses such as fact-checking and public announcements [10].

Butts, Bollman, and Murillo (2023) present a model evaluating the effectiveness of disinformation mitigation policies through simulations that demonstrate how interventions like account bans or content labeling may reduce the spread of false information [11].

John Lang (2016) models behavioral responses in networks by incorporating social factors into decision-making, creating opportunities to integrate normative and regulatory influences into such models [12].

Cristina Francalanci and colleagues (2015) study how power-law distributions reflect imbalances in information dissemination, suggesting that influence-driven dynamics could be moderated through network design or regulatory frameworks [13].

Collectively, these studies form a multidisciplinary foundation for developing models that synthesize legal theory with mathematical modeling. They suggest that legal constraints can be introduced into information diffusion models via system parameters such as compliance thresholds, probabilistic enforcement, or behavioral nudges. Incorporating regulatory norms into models of information diffusion

is essential for building robust frameworks to better understand, simulate, and ultimately manage information dynamics in regulated digital environments [14, 15, 16].

3. Development of a mathematical model

There are many different variants of mathematical approaches to creating models, because all models in one way or another use different variables to calculate the corresponding weighting coefficients and parameters. As one of the variants of the mathematical model that describes the compromise between freedom of speech and ensuring public security and national interests when regulating information influences in social networks. The model is formulated as an optimization problem in which the choice of the "intensity of regulation" (denoted by R) affects both the level of freedom of speech and the level of security and protection of national interests.

The first variable for the future mathematical model is the level of regulation as R (where $R \in [0, 1]$) is a parameter characterizing the intensity of the application of measures (no regulation at $R = 0$ to maximum regulation at $R = 1$).

The freedom of speech index should depend on the level of regulation. Let us denote it as F(R). For, F(R) we propose the following dependence:

$$F(R) = 1 - R^{\gamma}, \tag{1}$$

where $\gamma > 0$ is the coefficient that determines how quickly the loss of freedom of speech increases with increasing levels of regulation.

The public safety index should also depend on the level of regulation. Let us denote it as $S(R)$. Since even without additional security measures there can be a certain basic level S_0, we propose:

$$S(R) = S_0 + (S_{max} - S_0) \cdot (1 - e^{-k_S R}), \tag{2}$$

where S_0 – basic level of security (at R=0), $S_{max} \in (S_0, 1]$ – the maximum level of safety that can be approached with increasing regulation, $k_S > 0$ – a parameter that determines the growth rate of the security index.

After the public security index, we introduce the index of protection of national interests, which we will denote by $N(R)$. $N(R)$ we define it similarly to (2):

$$N(R) = N_0 + (N_{max} - N_0) \cdot (1 - e^{-k_N R}), \tag{3}$$

where N_0 – basic level of protection of national interests (at R=0), $N_{max} \in (N_0, 1]$ – the maximum possible level of protection of national interests, which can be approached with increasing regulation, $k_N > 0$ – growth rate.

Let us consider in more detail S_{max}. If maximum regulation provides almost complete security, we can take and $S_{max} = 1$. However, if security cannot reach an ideal level even with maximum regulation (for example, due to the impossibility of complete control over information flows) or it is necessary to model a more realistic case where even the most stringent measures do not provide absolute security, then we can choose , for $S_{max} < 1$ example $S_{max} \approx 0.95$, to take into account residual risks. The same is also true for N_{max}.

And perform the interpretation k_S. When small k_S (for example, $k_S \approx 0.5 \ldots 1$), safety increases slowly with an increasing regulation level R, i.e., a significant increase in regulation is required to significantly improve safety. Whereas, if k_S large (for example, $k_S \approx 3 \ldots 5$), safety quickly reaches its maximum even with a small regulation level R, i.e., a small increase in regulation significantly improves safety.

To determine k_S in practical application. The first is to analyze real data. If there is statistical data on the relationship between the level of regulation (for example, limiting disinformation) and the level of public safety (reducing social tension or reducing the number of offenses), it can be selected k_S by approximating empirical data.

Secondly, it is an expert assessment of the impact of the regulation on the relevant safety. If the regulation has a negligible effect on safety, a smaller one is chosen k_S (for example, from 0.5 to 1). If the effect is very significant, a larger one is chosen k_S (for example, from 3 to 5).

Optimization methods are then used to select the one k_S that best matches historical data or expected security behavior [17, 18].

For a clearer understanding, let us define a specific case for k_S by formula (2) (the same is true for (3)). Let us assume that the initial level of safety is $S_0 = 0.5$, and the maximum level is $S_{max} = 0.95$. If the regulation is very effective and provides 90% of the safety gain already at $R = 0.5$, then k_S can be about 3 (since $e^{-3 \cdot 0.5} \approx 0.22$, which quickly reduces the residual safety gain). If the regulation effect is weaker, and at $R = 0.5$ safety increases only to 0.7, then $k_S \approx 1$(since $e^(- 1 \cdot 0.5) \approx 0.61$, i.e. the decline occurs more slowly).

This confirms that the value k_S depends on real-world conditions and must be determined through modeling or data analysis.

Another important part of the mathematical model of legal regulation is the intensity of harmful informational influences. Let us denote it as I(normalized value from 0 to 1). Regulation reduces effective harm, so let us introduce the effective level of harm:

$$I_{ef}(R) = I \cdot (1 - R), \tag{4}$$

where $I \in [0, 1]$ — the initial level of harmful information impact (for example, the level of disinformation or propaganda without regulation), $I_{ef}(R)$ — the residual level of information threat after the introduction of a certain level of regulation.

If we consider partial cases, then in the case when there is no regulation $(R = 0)$, then $I_{ef}(0) = I \cdot (1 - 0) = I$, that is, the entire harmful information impact remains unchanged. Conversely, if the regulation is maximum $(R = 1)$, then $I_{ef}(1) = I \cdot (1 - 1) = 0$, which means the complete elimination of the information threat.

At intermediate values, R the threat level decreases linearly with the level of interference. This formula shows that with increasing regulation, the level of information threat decreases.

The initial level of harmful information impact I is a quantitative assessment of the level of disinformation, propaganda, or other undesirable information phenomena in social networks before the application of any legal regulation $(R = 0)$ to automatically analyze the level of harmful information impact I and dynamically adjust it in accordance with the level of security $S(R)$ and protection of national interests $N(R)$. Such methods allow assessing the content of publications and determining the level of their threat to public security and national interests.

Content assessment is performed using NLP models that analyze the use of words or phrases associated with calls for violence, hate speech, threats, or disinformation. Using classification models such as deep neural networks or statistical analysis methods, the risk level of the content is determined $I_{ef}(R)$. In this case, regulation R affects the probability of distribution of such content, gradually reducing its effectiveness.

When assessing the threat through text, formula (4) for $I_{ef}(R)$ takes on certain changes:

$$I_{ef}(R) = I(x) \cdot (1 - R), \tag{5}$$

where x — the text of the publication, $P(x)$ — the probability that the text is malicious.

$$I(x) = P(x) \cdot I_{max}, \tag{6}$$

Formula (6) shows the contribution of the text to the overall information threat.

If such a model identifies the text as malicious with probability 0.8, then the initial level is $I_x = 0.8$, and after adjustment $(R = 0.3)$ the effective level is $I_{ef}(R) = 0.8(1 - 0.3) = 0.56$.

User history is an additional risk factor that can increase the initial value I. If a user has previously repeatedly violated the platform policy or spread misinformation, their content may receive a higher level of risk $I_{ef}(R)$. The impact of this factor can be expressed through a function of the user's history

of actions, which is integrated into the model for calculating the overall information threat. In this case, formula (5) takes on a slightly different form, taking into account the user history indicator:

$$I_{ef}(R, u) = I(x) \cdot (1 - R) \cdot (1 + H(u)), \tag{7}$$

where H(u)— user violation history (number of previous blocks, normalized to $[0, 1]$).

If the user has 5 previous violations, then $H(u) = 0.5$, which increases the risk by 50%. For example, if $I_{ef}(R) = 0.56$, then considering the history of the user's violations, $I_{ef}(R)$ it increases significantly: $I_{ef}(R, u) = 0.561.5 = 0.84$. But this approach requires the creation of a certain database, into which the data on the violations of individual users will be entered.

Content analysis for disinformation is based on fact-checking using knowledge bases, which allows assessing the correspondence of statements on social networks to real events. In the case of detection of fake information, its contribution to the level of information threat I increases, which may require an increase in the level of regulation R to achieve an acceptable level of security $S(R)$ and protection of national interests $N(R)$.

For calculations, we introduce a variable that shows the misinformation of the text:

$$D(x) = 1 - similarity(x, fact), \tag{8}$$

where x — the text of the publication, $similarity(x, fact)$ — similarity of the statement with the base of verified facts, $D(x)$ determines the level of information distortion (the greater the $D(x)$, the greater the risk). In this case, the original formula (5) will receive new input data for calculations:

$$I_{ef}(R) = I(x) \cdot (1 - R) \cdot (1 + D(x)). \tag{9}$$

If the similarity with the fact is 0.2, then $D(x) = 1 - 0.2 = 0.8$, which greatly increases the risk level. When the indicator of misinformation of the text is neglected, the residual level of information threat is equal to $I_{ef}(R) = 0.56$, but after considering misinformation $I_{ef}(R) = 0.56 \cdot 1.8 = 1.01$.

Geolocation analysis allows you to identify potentially risky content depending on its location. If the content comes from regions of increased information threat or geopolitical conflicts, the likelihood of its manipulative nature increases, which affects the initial value of the information threat I. Geolocation data can be used as one of the factors in the function of determining the level of security $S(R)$.

Geolocation risk indicator $G(l)$ can take on two meanings: either 1, if the content l was posted from a region that belongs to the list of regions with a potential threat, or 0, if the content lwas posted from a region that does not belong to the list of regions with a potential threat:

$$G = \begin{cases} 1, & l \in \text{conflict zone} \\ 0, & \text{otherwise} \end{cases} \tag{10}$$

When considering, $G(l)$ formula (6) takes the following form:

$$I_{ef}(R, l) = I(x) \cdot (1 - R) \cdot (1 + G(l)). \tag{11}$$

It is worth noting that a gradient scale can be used to assess the risk of content based on geographical location, which considers the distance from the conflict zone. Such a scale allows for a dynamic assessment of the risk level $G(l)$ based on its location, rather than simply setting it to 0 or 1, which was chosen for the simplicity of the example.

With gradient estimation, formula (10) for $G(l)$, will take on a new form - exponential decay, ensuring a slow reduction in risk with distance from the conflict zone:

$$G(d) = e^{-k_d \cdot d(l, l_c)}, \tag{12}$$

where $G(l)$ — risk level at point l, $d(l, l_c)$ — distance from the content location l to the nearest conflict zone l_c, $[d(l, l_c)] = [km]$, k_d — the coefficient of risk decline with increasing distance (the larger k_d, the faster the impact decreases).

Based on formula (12) and the list of distances in kilometers, we can create an approximate gradient scale table for our study, which can be used without formula (12), and analytically select the necessary data:

Table 1
Risk Scales Depending on Distance to the Conflict Zone

Distance to the conflict zone $d(l, l_c)$, km	Risk level $G(l)$
$d = 0$ (in the conflict zone)	1.00
$d < 10$	0.90
$10 \leq d < 30$	0.75
$30 \leq d < 50$	0.60
$50 \leq d < 100$	0.40
$100 \leq d < 200$	0.25
$200 \leq d < 500$	0.10
$d \geq 500$	0.05

This scale table works as follows:

1. Content published in the very epicenter of the conflict $(d = 0)$ receives maximum risk $(G(l) = 1)$.

2. At up to 10 km, the risk is still high $(G(l) = 0.9)$, as the information may be related to the conflict.

3. At 50–100 km, the risk is significantly reduced, as the possibility of direct contact with the conflict is less.

If the content is published at more than 500 km, its connection with the conflict situation is unlikely, but still not equal to 0 $(G(l) = 0.05)$.

However, for this software implementation, if you want a fast reduction in risk with distance, you can increase it k_d (for example, to 0.01). Conversely, if you want a slower reduction, you should decrease it k_d (for example, to 0.002).

The context of events is also an important factor in modeling the level of threat. Information posted during critical events, such as elections or social unrest, has an increased risk of manipulation and disinformation, which affects the function of changing security $S(R)$ and information threat $I_{ef}(R)$. Considering the time factor allows you to dynamically adjust the level of control R, ensuring that measures are appropriate to the current situation.

Consider the increased risk during periods of critical events, which we $C(t)$ can denote using an exponential decay function like (13):

$$C(t) = e^{-k_C \cdot (t - t_0)}, \tag{13}$$

where $C(t)$ – risk weighting coefficient depending on time; t_0 – the moment of the beginning of critical events; k_C – the rate of decline in the impact of events.

The graph obtained based on this code will show how the risk of an event decreases over time. That is, at low k_C the risk remains significant for a long time. Conversely, with high k_C the risk decreases rapidly after the peak of the event.

When considering $C(t)$ formula (5) takes the formula (11) with the exception that instead of $G(l)$ we use $C(t)$:

$$I_{ef}(R, l) = I(x) \cdot (1 - R) \cdot (1 + C(t)). \tag{14}$$

Thus, the integration of all the above factors into a mathematical model allows for a dynamic approach to regulating information flows in social networks. Regulation R is defined as a function of the risk of information impact Iand the level of threat to security $S(R)$ and national interests $N(R)$, which allows achieving the optimal balance between protecting society and preserving freedom of speech.

After obtaining all the necessary intermediate data, you can proceed to calculate the national security index:

$$NSL(R) = S(R) + N(R) - \delta I_{ef}(R), \tag{15}$$

where $NSL(R)$ — the overall level of national security at the level of regulation R, $S(R)$ — the level of public safety, obtained from formula (2), $N(R)$ — the level of protection of national interests, obtained from formula (3), $I_{ef}(R)$ — the residual level of information threat, obtained from formulas (4, 5), $\delta > 0$ — the weight coefficient of the impact of an information threat on national security (determines how much harmful information affects the overall level of security).

Formula (15) works as follows. The positive effects of regulation $S(R)$ and are added $N(R)$, which increase with increasing regulation R, since more controlled space improves public safety and state protection.

The negative effect of the information threat is subtracted $I_{ef}(R)$, which decreases as R, but still has a negative impact. This negative impact is scaled by a factor δ (for example, if disinformation has a serious impact on security, δ it will be large).

Regarding interpretation δ, the following can be said:

If δ it is small ($\delta \approx 0.1$), the information threat has a weak impact on security. This may mean that society has a high level of resilience to disinformation, or that other factors (economy, military power) have a greater impact on security.

If δ the average ($\delta \approx 0.5$), the information threat is an important but not a determining factor. For example, in a country with strong media and a developed fact-checking system, information attacks can be a serious problem, but not destructive.

If δ large ($\delta \geqslant 1$), the information threat has a critical impact on national security. This may be typical of situations where fake news, propaganda, or cyberattacks can cause mass panic, political destabilization, or even leading to social unrest.

Let's consider an example using selected numerical values.

Let's assume that public safety $S(R) = 0.7$, protection of national interests $N(R) = 0.6$, information threat after regulation $I_{ef}(R) = 0.5$, Let's consider three options δ, we list them in Table 2.

Table 2
Comparison $NSL(R)$ for Different δ.

δ	Impact of information threat	$NSL(R)$ (national security)
0.1	Weak	0.7+0.6-0.1×0.5=1.25
0.5	Moderate	0.7+0.6-0.5×0.5=1.0
1.0	Critical	0.7+0.6-1.0×0.5=0.8

Table 2 shows that if δ it is small, national security is almost unchanged by disinformation. If δ it is large, even a moderate level of information threat can significantly reduce security.

If we choose δ for a real situation, then in countries with strong information hygiene ($\delta \approx 0.1 - 0.3$), disinformation has a weak impact. In countries with hybrid warfare, low levels of trust in the media ($\delta \approx 0.5 - 0.8$), information attacks can seriously affect security.

In situations of crisis or information warfare ($\delta \geqslant 1$), even one massive fake can have catastrophic consequences.

Based on the above data and calculations, we see that the coefficient δ determines how sensitive national security is to information threats. It should be adjusted depending on the level of media literacy of the population, information attacks, and the socio-political situation.

Returning to formula (15), it is true for this formula that if R is small, then the level of safety $NSL(R)$ will be low due to the high influence of $I_{ef}(R)$.

If R it increases, then $S(R)$ they $N(R)$ grow, and if $I_{ef}(R)$ it decreases, then it increases $NSL(R)$.

If the coefficient δ is large, it means that the information threat has a critical impact on national security, and even a small residual level $I_{ef}(R)$ can significantly reduce $NSL(R)$.

To reflect the trade-off between the different components, we introduce a balance index $B(R)$, which is a weighted sum of three indices:

$$B(R) = w_F \cdot F(R) + w_S \cdot S(R) + w_N \cdot N(R), \tag{16}$$

where $w_F > 0$ — the weight of freedom of speech $F(R)$, $w_S > 0$ — the importance of public safety $S(R)$, $w_N > 0$ — the importance of protecting national interests $N(R)$, $w_F + w_S + w_N = 1$ — normalization of weight coefficients.

This model allows us to reflect the priorities of society and/or government in matters of information regulation.

Let's consider certain cases of weighting factors and their meanings.

For the first case, we will choose a high value w_F (i.e., the priority of freedom of speech). If $w_F \approx 0.6 \ldots 0.8$, and w_S, w_N are respectively small, this means that freedom of speech is the main social priority for this state. At the same time, regulation R should be minimal to avoid censorship. And even if the level of information threats is high, society is ready to take risks to preserve a free information space. As an example, we can cite liberal democracies (such as the USA or the EU zone), where freedom of speech is a key value.

For the second case, we will choose a high value w_S (priority of public safety). If $w_S \approx 0.5 \ldots 0.7$, then this means that for this state the main goal is to prevent internal threats, such as social conflicts, violence, terrorist attacks. At the same time, information that incites crimes or contributes to radicalization must be strictly controlled. In this case, temporary restrictions on freedom of speech are possible for the sake of protecting society. As an example, we can cite countries that are fighting terrorism, such as France after the terrorist attacks of 2015, or states in conditions of political instability.

And for the third case, consider a high value w_N(priority of national interests).

If $w_N \approx 0.5 \ldots 0.8$, this means that in this state there is a focus on protection from external threats, such as propaganda, information wars, and espionage. Also, in a country with such a system, w_N strict measures have been created against foreign information campaigns, as well as possible blocking or restriction of content that harms the state. As an example, we can show Ukraine during the war (blocking Russian channels and propaganda) and China (content filtering to control public opinion).

However, these three individual cases have a specific bias towards one or another's weight coefficient. To solve the problem, it is worth choosing the optimal weights w_F, w_S, w_N. For this, we offer three ready-made models:

A model for democracy (strong freedom of speech, medium security controls) with minimal regulation of information.

$$w_F = 0.6, w_S = 0.2, w_N = 0.2. \tag{17}$$

National security model (medium freedom of speech, strong security control). The balance between protection and freedom is maintained.

$$w_F = 0.3, w_S = 0.4, w_N = 0.3. \tag{18}$$

Authoritarian control model (strong censorship, priority of state interests). Here, maximum control of information occurs.

$$w_F = 0.1, w_S = 0.4, w_N = 0.5. \tag{19}$$

However, these three models are only examples, and of course the choice of weighting factors depends on the specific policy of the state and the level of threats. In conditions of war or crisis, freedom of speech may temporarily give way to security and national interests.

The balance index (16) is the last element of the theoretical description of this mathematical model. And in general, the mathematical model of legal regulation of the spread of information influences social networks takes the following form:

Index functions:

$$
\begin{aligned}
F(R) &= 1 - R^{\gamma}, \\
S(R) &= S_0 + (S_{\max} - S_0)\left(1 - e^{-k_S R}\right), \\
N(R) &= N_0 + (N_{\max} - N_0)\left(1 - e^{-k_N R}\right), \\
I_{\text{ef}}(R) &= I \cdot (1 - R), \\
NSL(R) &= S(R) + N(R) - \delta \cdot I_{\text{ef}}(R).
\end{aligned}
\tag{20}
$$

Balance index:

$$
B(R) = w_F F(R) + w_S S(R) + w_N N(R). \tag{21}
$$

Optimization problem:

$$
\begin{aligned}
&\text{Max: } B(R), \quad R \in [0,1], \\
&\text{under the conditions: } F(R) \geq F_{\min}, \quad NSL(R) \geq NSL_{\min}.
\end{aligned}
\tag{22}
$$

By adjusting the parameters (γ, k_S, k_N, S_0, S_max, N_0, N_max, δ, I, as well as the weighting factors w_F, w_S, w_N) it is possible to adapt the model to specific conditions, societal priorities and current threats. We obtain a tool that can help legislators and experts in determining the optimal level of legal regulation to achieve a balance between fundamental rights and ensuring national security.

4. Formulation of the optimization problem

After creating the theoretical basis of the mathematical model, we proceed to verify it on practical data. To do this, we set the task: to find the optimal level of regulation R^* and the corresponding index values such that the balance index $B(R)$ is maximized, and the levels of freedom of speech and national security do not fall below the specified minimum threshold values.

If we formalize this into a mathematical formula, we get the following:

$$
\begin{aligned}
&\text{Find } R^* \in [0,1], \text{ which maximizes } B(R), \\
&\quad \text{under the conditions:} \\
&\quad F(R) \geq F_{\min}, \\
&\quad NSL(R) \geq NSL_{\min}.
\end{aligned}
\tag{23}
$$

That is:

$$
R^* = \arg\max B(R) \quad \text{subject to } F(R) \geq F_{\min}, \text{and} \quad NSL(R) \geq NSL_{\min}. \tag{24}
$$

For illustration, we perform parameterization using the following values (all normalized to $[0,1]$):

- Freedom of speech index parameter: $\gamma = 1$ (linear dependence: $F(R) = 1 - R$),
- Security index parameters: $S_0 = 0.5$, $S_{\max} = 1$, $k_S = 2$ (i.e. $S(R) = 0.5 + 0.5(1 - e^{-2R})$),
- National interest index parameters: $N_0 = 0.5$, $N_{\max} = 1$, $k_N = 2$ (i.e. $N(R) = 0.5 + 0.5(1 - e^{-2R})$),
- Harmful informational influence: $I = 0.8$,
- Damage coefficient: $\delta = 0.5$,
- Weighting factors: $w_F = 0.4$, $w_S = 0.3$, $w_N = 0.3$,
- Threshold values: $F_{\min} = 0.7$, $NSL_{\min} = 0.9$.

We perform calculations according to the selected parameters:
So the index of freedom is:

$$F(R) = 1 - R \quad (\gamma = 1). \tag{25}$$

Safety index:

$$S(R) = 0.5 + 0.5(1 - e^{-2R}). \tag{26}$$

National interest index:

$$N(R) = 0.5 + 0.5(1 - e^{-2R}). \tag{27}$$

Effective harmfulness of information:

$$I_{\text{ef}}(R) = 0.8 \cdot (1 - R). \tag{28}$$

National security index:

$$NSL(R) = S(R) + N(R) - 0.5 \cdot I_{\text{ef}}(R). \tag{29}$$

Integral balance:

$$\begin{aligned} B(R) = 0.4(1 - R) + 0.3 \left[0.5 + 0.5(1 - e^{-2R})\right] + \\ + 0.3 \left[0.5 + 0.5(1 - e^{-2R})\right]. \end{aligned} \tag{30}$$

After creating the theoretical basis of the mathematical model, we will proceed to verify it on practical data. To do this, we will set the task: to find the optimal level of regulation R^* and the corresponding index values, such that the balance index $B(R)$ is maximum, and the levels of freedom of speech and national security do not fall below the specified minimum threshold values.

If we formalize this into a mathematical formula, we get the following:

$$\begin{aligned} &\text{Find } R^* \in [0, 1], \text{ which maximizes } B(R), \\ &\text{under the conditions:} \\ &F(R) \geq F_{\min}, \\ &NSL(R) \geq NSL_{\min}. \end{aligned} \tag{23}$$

That is:

$$R^* = \arg\max B(R) \quad \text{subject to } F(R) \geq F_{\min} \text{ and } NSL(R) \geq NSL_{\min}. \tag{24}$$

For illustration, we perform the parameterization using the following values (all values are normalized to $[0, 1]$):

1. Parameters of the freedom of speech index: $\gamma = 1$ (linear dependence: $F(R) = 1 - R$).
2. Security index parameters: $S_0 = 0.5$, $S_{\max} = 1$, $k_S = 2$ (i.e., $S(R) = 0.5 + 0.5(1 - e^{-2R})$).
3. Parameters of the national interest index: $N_0 = 0.5$, $N_{\max} = 1$, $k_N = 2$ (i.e., $N(R) = 0.5 + 0.5(1 - e^{-2R})$).
4. Harmful informational influence: $I = 0.8$.
5. Damage coefficient: $\delta = 0.5$.
6. Weighting factors: $w_F = 0.4$, $w_S = 0.3$, $w_N = 0.3$.
7. Threshold values: $F_{\min} = 0.7$ and $NSL_{\min} = 0.9$.

We perform calculations according to the selected parameterization values. So the index of freedom is:

$$F(R) = 1 - R \quad (\gamma = 1). \tag{25}$$

Safety index:

$$S(R) = 0.5 + 0.5(1 - e^{-2R}). \tag{26}$$

National Interest Index:

$$N(R) = 0.5 + 0.5(1 - e^{-2R}). \tag{27}$$

Effective harmfulness of information:

$$I_{\text{ef}}(R) = 0.8 \cdot (1 - R). \tag{28}$$

National Security Index:

$$NSL(R) = S(R) + N(R) - 0.5 \cdot 0.8 \cdot (1 - R). \tag{29}$$

Integral balance:

$$B(R) = 0.4 \cdot (1 - R) + 0.3[0.5 + 0.5(1 - e^{-2R})] + 0.3[0.5 + 0.5(1 - e^{-2R})]. \tag{30}$$

Finding the optimal one R^* is done by calculating the derivative dB/dR, setting the condition $dB/dR = 0$ (taking into account additional restrictions $F(R) \geq F_{\min} \Rightarrow F(R) \geq 0.7$ (i.e., freedom of speech should not fall below 70% of the maximum) and $NSL(R) \geq NSL_{\min} \Rightarrow NSL(R) \geq 0.9$ (national security must be at least 90%).

With this interpretation, with an increase, R and $N(R)$ increase $S(R)$ (because measures to filter harmful influences are strengthened, control over the information space is increased), but decreases $F(R)$, because restrictions that may affect freedom of speech are strengthened.

Determining the optimal value R^* provides a compromise — a sufficient level of security and protection of national interests is achieved, while freedom of speech does not fall below the minimum permissible level.

National security $NSL(R)$ considers both the positive effect of increasing $S(R)$ and $N(R)$ and the negative impact of residual harmfulness $I_{\text{ef}}(R)$. The condition is that $NSL(R)$ exceeds a certain critical threshold $NSL_{\min}$.

Let's consider a few examples of calculations for different values R (numerical values are approximate), we list them in Table 3.

Table 3
Examples of Calculations

Variables	$R = 0$	$R = 0.2$	$R = 0.3$
Freedom of speech, $F(R)$	1.000	0.800	0.700
Security, $S(R)$	0.500	0.66485	0.7256
National interests, $N(R)$	0.500	0.66485	0.7256
Effective harmfulness, $I_{\text{ef}}(R)$	0.800	0.640	0.560
National Security, $NSL(R)$	0.600	1.0097	1.1712
Balance, $B(R)$	0.700	0.719	0.7154

Let's analyze the calculated values according to the conditions.

Threshold of freedom of speech $F(R) \geq 0.7$: since $F(R) = 1 - R$, then this condition is fulfilled when $R \leq 0.3$.

National security threshold $NSL(R) \geq 0.9$:

According to calculations:

We accept $NSL(0) = 0.6$ ($R = 0$ not allowed).

At $R = 0.2$, $NSL(0.2) \approx 1.01$ (condition is met).

At $R = 0.3$, $NSL(0.3) \approx 1.17$.

Thus, the permissible range R is from approximately 0.15–0.2 (the lower limit is determined by the need to achieve $NSL \geq 0.9$) to 0.3 (the upper limit from the condition $F \geq 0.7$).

According to the data obtained, we will make the optimal choice R.

The value of the balance index $B(R)$ for the points considered:

$B(0) = 0.7$, $B(0.2) \approx 0.719$, $B(0.3) \approx 0.715$.

From the calculations the greatest value $B(R)$ is obtained when $R \approx 0.2$.

According to this model and parameters that can be adapted to Ukrainian realities, the optimal level of regulation is $R^* \approx 0.2$, which means that the "regulation intensity" should be about 20%. In this case, we get:

Freedom of speech: $F(0.2) = 0.8$ (80% of the maximum, exceeding the 70% threshold).

Public safety: $S(0.2) \approx 0.665$.

Protection of national interests: $N(0.2) \approx 0.665$.

National Security: $NSL(0.2) \approx 1.01$ (above 0.9).

Balance index: $B(0.2) \approx 0.719$ – the maximum among the permissible options.

Thus, considering the compromise between preserving freedom of speech and ensuring national security, the optimal regulation for Ukraine under this model is approximately 20%.

5. Conclusions

The conducted research underscores the importance of developing an integrated legal framework capable of effectively regulating information flows in social networks, while taking into account digital dynamics and emerging technical risks. The proposed mathematical model demonstrates how regulatory intensity can be quantitatively linked to key societal indicators such as freedom of speech, public safety, and national security. Through optimization of regulatory parameters based on measurable criteria, policymakers can avoid the extremes of both excessive censorship and uncontrolled information disorder.

However, it is essential to emphasize that the current version of the model remains primarily theoretical. No empirical data from real-world social networks were incorporated into this study, and all simulations were performed using hypothetical scenarios. This limitation is explicitly acknowledged. Future research efforts should focus on empirical validation using open-source or synthetic datasets and further adaptation of the model to reflect specific socio-cultural and legal environments.

Such developments are critical for advancing the practical application of mathematical models in digital policymaking, allowing legislators to establish regulation levels that strike a sustainable balance between the protection of fundamental rights and the safeguarding of national security in the digital era.

Declaration on Generative AI

The authors have not employed any Generative AI tools.

References

[1] J. S. Al-Azzeh, M. A. Hadidi, R. S. Odarchenko, S. Gnatyuk, Z. Shevchuk, Z. Hu, Analysis of self-similar traffic models in computer networks, International Review on Modelling and Simulations 10 (2017) 328–336. doi:10.15866/iremos.v10i5.12009.

[2] O. S. Ulichev, Model and methods of spreading information influences in social networks in conditions of information confrontation, Ph.D. thesis, National Aviation University, Kyiv, 2021. Dissertation for the degree of Candidate of Technical Sciences, specialty 21.05.01 “Information Security of the State”.

[3] J. Dhar, A. Jain, V. K. Gupta, A mathematical model of news propagation on online social network and a control strategy for rumor spreading, Social Network Analysis and Mining 6 (2016) 57. doi:10.1007/s13278-016-0366-5.

[4] M. Muhlmeyer, S. Agarwal, Information Spread in a Social Media Age: Modeling and Control, 1st ed., CRC Press, 2021. doi:10.1201/9780429263842.

[5] Y. V. Nakonechna, Mathematical models of the dynamics of the spread of cases of information concealment in social networks, Theoretical and Applied Cybersecurity 1 (2019) 41–47. doi:10.20535/tacs.2664-29132019.1.169082.

[6] P. V. Khrapov, V. A. Stolbova, Mathematical modeling of the news spreading process in social networks, Modern Informational Technologies and IT Education (2019).

[7] M. Shur-Ofry, G. Fibich, The diffusion of legal innovation—insights from mathematical modeling, Cornell International Law Journal 52 (2019). URL: https://ww3.lawschool.cornell.edu/research/ILJ/upload/Shur-Ofry-final.pdf.

[8] W. Huleihel, Y. Refael, A mathematical framework for online social media auditing, Journal of Machine Learning Research 25 (2024). URL: http://www.jmlr.org/papers/volume25/22-1112/22-1112.pdf.

[9] L. Zhu, G. Guan, Z. Zhang, Mathematical analysis of information propagation model in complex networks, International Journal of Modern Physics B 34 (2020). doi:10.1142/S0217979220502409.

[10] A. E. Bhih, Z. Yaagoub, M. Rachik, K. Allali, Controlling the dissemination of rumors and anti-rumors in social networks, The European Physical Journal Plus 139 (2024). doi:10.1140/epjp/s13360-023-04844-y.

[11] D. J. Butts, S. A. Bollman, M. S. Murillo, Mathematical modeling of disinformation and effectiveness of mitigation policies, Scientific Reports 13 (2023). URL: https://www.nature.com/articles/s41598-023-45710-2.pdf.

[12] J. Lang, Mathematical Modelling of Social Factors in Decision Making Processes, Master's thesis, University of Waterloo, 2016. URL: https://uwspace.uwaterloo.ca/bitstream/handle/10012/10627/Lang_John.pdf?sequence=5.

[13] C. Francalanci, A. Hussain, F. Merlo, Representing social influencers and influence using power-law graphs, Mathematics & Information Modeling (2015). URL: https://re.public.polimi.it/bitstream/11311/981448/4/Representing%20Social%20Influencers%20and%20Influence_11311-981448_Francalanci.pdf.

[14] Y. Averyanova, et al., UAS cyber security hazards analysis and approach to qualitative assessment, in: S. Shukla, A. Unal, J. V. Kureethara, D. Mishra, D. Han (Eds.), Data Science and Security, volume 290 of *Lecture Notes in Networks and Systems*, Springer, Singapore, 2021, pp. 258–265. doi:10.1007/978-981-16-4486-3_28.

[15] O. Tkachenko, A. Ilienko, O. Ulichev, Y. Meleshko, L. Halata, Modern studies of information influence in social networks, Cybersecurity: Education, Science, Technique 3 (2025) 120–140. doi:10.28925/2663-4023.2025.27.716.

[16] O. Tkachenko, A. Ilienko, O. Ulichev, Y. Meleshko, O. Smirnov, Legal foundations of information influence dissemination in social networks, Cybersecurity: Education, Science, Technique 2 (2024) 170–188. doi:10.28925/2663-4023.2024.26.685.

[17] R. Kostyrko, T. Kosova, L. Kostyrko, L. Zaitseva, O. Melnychenko, Ukrainian market of electrical energy: Reforming, financing, innovative investment, efficiency analysis, and audit, Energies 14 (2021) 5080. doi:10.3390/en14165080.

[18] Z. Hu, S. Gnatyuk, T. Okhrimenko, S. Tynymbayev, M. Iavich, High-speed and secure prng for cryptographic applications, International Journal of Computer Network and Information Security 12 (2020) 1–10. doi:10.5815/ijcnis.2020.03.01.